

הגדרה: חבורה פ נקראת וכלית אם $\forall a, b \in G: ab=ba$

קבוצה:

(1) $(\mathbb{Z}, +)$ וכלית

$(GL_n(\mathbb{F}), \cdot)$ חבורה. \mathbb{F} וכלית
מטריצות
היציבות

תכונות:

תהי G חבורה, נק שלכל $a \in G$ מתקיים $a^2=e$. הוכיחו e וכלית.

הוכחה:

נסתכל על $abbaba$

$$ba = ae \cdot a \cdot ba = abbaba = ab(ba)^2 = ab \cdot e = ab$$

הגדרה: תהי G חבורה. המרכז של G $Z(G) = \{a \in G: \forall b \in G, ab=ba\}$

send

$$Z(GL_n(\mathbb{F})) = \{\alpha I: \alpha \neq 0 \in \mathbb{F}\}$$

הגדרה: תהי G חבורה ו $H \subseteq G$ נגיד H תת-חבורה

של G ונסמן $H \subseteq G$, אם היא חבורה ביחס לאותן פעולות

קריטריון מקוצר:

H חבורה, $H \subseteq G$ אז H תת-חבורה אם

I $H \neq \emptyset$

II סגירות לפעולה

III סגירות לאינברסי

קולומס

$$H = n\mathbb{Z} \quad G = \mathbb{Z} \quad (1)$$

$$H = SL_n(\mathbb{F}) \quad G = GL_n(\mathbb{F}) \quad (2)$$

מטריצות
עם דטרמיננט 1

$$H = \{A \in GL_n(\mathbb{F}) \mid |A| = \pm 1\} \quad G = GL_n(\mathbb{F}) \quad (3)$$

תרגילים:

$$H = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\} \quad H \subseteq SL_3(\mathbb{R}) \quad \text{נוכחים:}$$

פתרון:

$$a = b = c = 0 \quad I \in H \quad (1)$$

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a'+a & b'+ac'+b \\ 0 & 1 & c'+c \\ 0 & 0 & 1 \end{pmatrix} \quad (2)$$

$$\begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix} \quad (3)$$

תרגילים:

$$Z(G) \subseteq G, \quad G \text{ סגור}, \quad \text{נוכחים}$$

פונקציה:

$$e \in Z(G) \quad I$$

$$(ab) \cdot c = a(bc) = a(cb) = (ac)b = (ca)b = c(ab) \quad c \in G \text{ 'ה' } \quad a, b \in Z(G) \text{ 'ה' } \quad II$$

$$ab = ba \quad b \in G \text{ 'ה' } \quad a \in Z(G) \quad III$$

$$\Downarrow \\ ba^{-1} = a^{-1}b$$

חבורת אוילר

השקרה יחידה \mathbb{N}

$$U_n \equiv \underbrace{U(\mathbb{Z}_n, \cdot)}_{\text{חיבור}}$$

קונטרה:

$$U_6 = ?$$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$$U_6 = \{1, 5\}$$

היחידה

$$(k, n) = 1 \Leftrightarrow k \in U_n \quad \text{יחידה } k \in \mathbb{N} > n$$

הוכחה:

$$k \in U_n \Leftrightarrow \exists t \in \mathbb{N} \text{ כגון } k \cdot t = 1 \pmod{n}$$

$$\Leftrightarrow \exists s \in \mathbb{Z} \text{ כגון } kt = sn + 1 \Leftrightarrow \exists t \in \mathbb{Z} \text{ כגון } kt - sn = 1$$

$$\Leftrightarrow \exists t \in \mathbb{Z} \text{ כגון } kt - sn = 1 \Leftrightarrow (k, n) = 1$$

(בכיוון ההפוך נשתמש במערכת המשוואות $kt - sn = 1$ ונראה כי יש פתרון חיובי)

תרגיל:

פתרו את המשוואה $67x = 1 \pmod{234}$ (מצאו את ההופכי של 67)

$$x \in \mathbb{Z}_{234}$$

פתרון:

$$234 = 67 \cdot 3 + 51 \Rightarrow 67 = 1 \cdot 51 + 10 \Rightarrow 51 = 5 \cdot 10 + 1 \Rightarrow 1 = 51 - 5 \cdot 10$$

$$10 = 67 - 51 \Rightarrow 1 = 51 - 5(67 - 51) = -5 \cdot 67 + 6 \cdot 51$$

$$51 = 234 - 3 \cdot 67 \Rightarrow 1 = -5 \cdot 67 + 6(234 - 3 \cdot 67) = -23 \cdot 67 + 6 \cdot 234 \Rightarrow x = 211$$

פונקצית אוילר:

הגדרה: $\varphi(n) = |\{u \mid u \perp n\}|$

$\varphi(p) = p-1$, $\varphi(p^k) = p^k - p^{k-1}$
גלגל גלגל

טענה:

$\varphi(nm) = \varphi(n) \cdot \varphi(m)$ אם $(n, m) = 1$

נסקנה

$\varphi(n) = \prod (p_i^{k_i} - p_i^{k_i-1}) = n \cdot \prod (1 - \frac{1}{p_i})$ $n = \prod p_i^{k_i}$

קונטרא:

$\varphi(60) = 60(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 16$

$\varphi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$

חבורות ציקליות:

תהי $\langle a \rangle$ חבורה ו- $a \in \mathbb{Z}$ חת החבורה הנוצרת על ידי a :

$\langle a \rangle = \{ \sum \alpha^k \mid k \in \mathbb{Z} \}$

$\langle a \rangle$ זקראת ציקלית אם קיים $a \in \mathbb{Z}$ כך ש $\langle a \rangle = \langle a \rangle$

הצרכים כל החבורה ציקלית היא אפסית

קונטרא:

(1) $(\mathbb{Z}, +)$ נוצרת על ידי 1 (גם על ידי -1)

(2) $(\mathbb{Z}_n, +)$ נוצרת על ידי 1

(3) $(\mathbb{Z}_n, +)$ נוצרת על ידי 2: 2, 4, 6, 8, 1, 3, 5, 7, 0

תרגילים:

ג. \mathbb{Z} ו- \mathbb{R} בחבורה את

$$\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \rangle = \left\{ \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$$

סדר של איבר:

תהי a בחבורה ו- $a \in G$ הסדר של a , מסומן

$$O(a) = \min \{ n \in \mathbb{N} : a^n = e \}$$

אם הקבוצה ריקה $O(a) = \infty$

הערה: $a^m = 1$ או $m \mid O(a)$

רשימו בהוכחה $O(a) = \langle \varphi \rangle$

מסקנה:

תהי a בחבורה, $n = |a|$ ו- a ציקלית \Leftrightarrow ה"ם ג- a

איבר מסדר n

תכונות:

יהיו a ו- b בחבורות H ו- K $(a, b) \in G \times H$

$$O(a, b) = [O(a), O(b)]$$

הוכחה:

הוכחה:

$$(a, b)^{[O(a), O(b)]} = (a^{[O(a), O(b)]}, b^{[O(a), O(b)]}) =$$

$$= (a^{O(a) \cdot k}, b^{O(b) \cdot k}) = ((a^{O(a)})^k, (b^{O(b)})^k) = (e, e)$$

$$(a, b)^k = (e, e)$$

מכאן שני. נניח ש:

$$(a^k, b^k) = (e, e)$$

פשוט $a^k = b^k = e \Leftrightarrow O(a) \mid k \wedge O(b) \mid k$

כבר $[O(a), O(b)] = \min \{ k : (a, b)^k = e \} \Leftrightarrow [O(a), O(b)] \leq k$

תרגיל:

הוכיחו שהחבורה $\mathbb{Z}_n \times \mathbb{Z}_n$ היא לא ביקולית

נוכחה:

$$|\mathbb{Z}_n \times \mathbb{Z}_n| = n^2$$

$$n(a,b) = (na, nb) = (0,0) \iff (a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$$

$$n \leq n(a,b) = 0$$

הצדקה: בחבורה סופית לכל איבר יש סדר סופי

תרגיל:

$$O(a) = O(a^{-1}) - e$$

פתרון:

$$O(a) = n \quad \text{אז} \quad a^n = e$$

$$(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$$

$$(a^{-1})^n = e \iff a^n = e$$

לכן קבוצת המסדרים הטבעיים שלחלקת a או a^{-1} יוצרת ש-לכה. הפרט יש לה את אותו מינימום אז שיהיו יקה בשניהם

תרגיל:

G חבורה. הוסיף אינסוף האיברים מסדר סופי מחוץ לתת חבורה?

משוואה:

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} \quad G = GL_n(\mathbb{R})$$

$$O(a) = 4 \quad O(b) = 3 \quad ab = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad (ab)^n = \begin{pmatrix} n & 1 \\ 0 & 1 \end{pmatrix}$$

סדר n הוא סופי

תרגיל:

אם G ובלתי אבזאן אז אוסף האיברים מספר סופי הוא תת חבורה
(אוסף האיברים מספר סופי) $\text{Fin}(G) = \{e\}$

פתרון:

I $e \in \text{Fin}(G)$

II סגירות לקופסי-ראינו $(\text{ord}(a) = \text{ord}(a^{-1}))$

III סגירות לכפל

$$\text{ord}(a) = n, \text{ord}(b) = m$$

$$(ab)^{nm} = ab \cdot \dots \cdot ab = a^{nm} b^{nm} = e^m \cdot e^n = e$$

למה:

$$\text{ord}(a^i) = \frac{\text{ord}(a)}{(\text{ord}(a), i)}$$

סקנה:

נניח G חבורה ציקלית מספר n או מס' היוצרים
של G הוא $\varphi(n)$

הוכחה:

היינו $a \in G, \text{ord}(a) = n$. לכל $g \in G$ $g = a^i$ לאישהו i

$$g = a^i \Leftrightarrow \text{ord}(g) = \frac{n}{(n, i)} \Leftrightarrow \text{ord}(g) = n \Leftrightarrow (n, i) = 1$$

תרגיל:

האם φ היא חבורה ציקלית?

תשובה:

$$U_8 = \{1, 3, 5, 7\} \quad 3^2 = 1 \quad 5^2 = 1 \quad 7^2 = 1 \quad 1^1 = 1$$

יון אינר מספר 4, ולכן לא ציקלית

הצגתה: תהי G חבורה ו- $A \subseteq G$

$$\langle A \rangle = \bigcap_{A \subseteq H \subseteq G} H$$

מת חבורה
שנוצרת על ידי A

היון קונקרטי

$$\langle A \rangle = \{ a_1^{i_1} \dots a_n^{i_n} : a_1, \dots, a_n \in A, i_j = \pm 1 \}$$

דוגמאות:

(1) $G = \mathbb{Z}$, $H = \{2, 3\}$, $\langle H \rangle = \mathbb{Z}$, $\forall \mathbb{Z} \subseteq H$ כי $1 = 3 - 2$

(2) $H = \{4, 6\}$, $\langle H \rangle = 2\mathbb{Z}$

(3) $H = \{a, b\}$, $\langle H \rangle = \{ \pm a \pm b \} \mathbb{Z}$

הסקר: $\langle H \rangle = \{ \pm at + \pm bt : t \in \mathbb{Z} \}$
 של a ו- b מתחלק ב- (a, b) , ובנוסף (a, b) הוא
 צורף לייצור של a ו- b

הצגתה: נקראות נוצרת סופית אם קיימת קבוצה סופית

$$A \subseteq G \text{ כן } \langle A \rangle = G$$

תרשים:

הוכחה: (ס, זמלא) על-נוצרת סופית

הוכחה:

נב"ש יש $A = \{ \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \}$ כן $\langle A \rangle = \mathbb{Q}$ זמלא

$$\langle A \rangle = \left\{ \frac{a_1^{k_1}}{b_1^{t_1}} \dots \frac{a_n^{k_n}}{b_n^{t_n}} \right\}$$

במנה של p ויבר בקבוצה יחזים לרובים רק האורמים
 הראשוניים משתתפים ב- $a_1 \dots a_n$ ו- $b_1 \dots b_n$ משתתפים רק
 מספר סוגי של ראשוניים. ניקח p ראשוני של p משתתף
 $\frac{1}{p} \in \mathbb{Q}$ זמלא A